RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: LAW-T02

The SolarWinds CISO Litigation and What It Means for Your InfoSec Program

MODERATOR:

Scott M. Giordano, Esq.
Partner and Co-Founder
The CISO Law Firm PLLC
linkedin.com/in/scottmgiordano

PANELISTS:

John Barker, Esq., CHC, CCEP, CHPC, CHRC
Partner and Co-Founder
The CISO Law Firm PLLC
linkedin.com/in/johnwbarkerii

John Bates, JD, AIGP, CISSP, CCSP
Senior Manager, Cybersecurity
Ernst & Young LLP
linkedin.com/in/john-bates-jd

John T. Bandler, Esq.
Principal & Founder
Bandler Law Firm PLLC
linkedin.com/in/johnbandler

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The information shared during this panel discussion is for general informational purposes only and does not constitute legal advice. No attorney-client relationship is formed by attending or participating in this discussion. The views expressed by the panelists are their own and do not necessarily reflect the opinions of their respective law firms, clients, or any affiliated organizations.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. The views expressed by the presenters are their own and not necessarily those of Ernst & Young LLP or other members of the global EY organization or The CISO Law Firm. These slides are for educational purposes only and are not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice. SCORE no. 26447-251US_2

The Panel

MODERATOR:

Scott M. Giordano, Esq.

Partner and Co-Founder
The CISO Law Firm PLLC
linkedin.com/in/scottmgiordano

PANELISTS:

John Bates, JD

Senior Manager, Cybersecurity
Ernst & Young LLP
linkedin.com/in/john-bates-jd

John Barker, Esq.

Partner and Co-Founder
The CISO Law Firm PLLC
linkedin.com/in/johnwbarkerii

John T. Bandler, Esq.

Principal & Founder
Bandler Law Firm PLLC
linkedin.com/in/johnbandler

Agenda

01

Why this matters

02

SolarWinds case chronology

03

Lessons learned for inside and outside counsel

04

Best practices after SolarWinds for inside and outside counsel

RSAC 2025 Conference

Why this matters

Key paradigms

Tough environment: CISOs have a very tenuous relationship with their employers.

Civil and criminal liability: CISOs face personal liability for obstructing regulatory investigations into a data breach event.

Document decisions: Maintain thorough records of all cybersecurity decisions and actions to provide transparency and legal protection.

Secure adequate insurance coverage: Verify that your role is covered under the company's directors and officers (D&O) liability insurance to protect against potential personal liability.

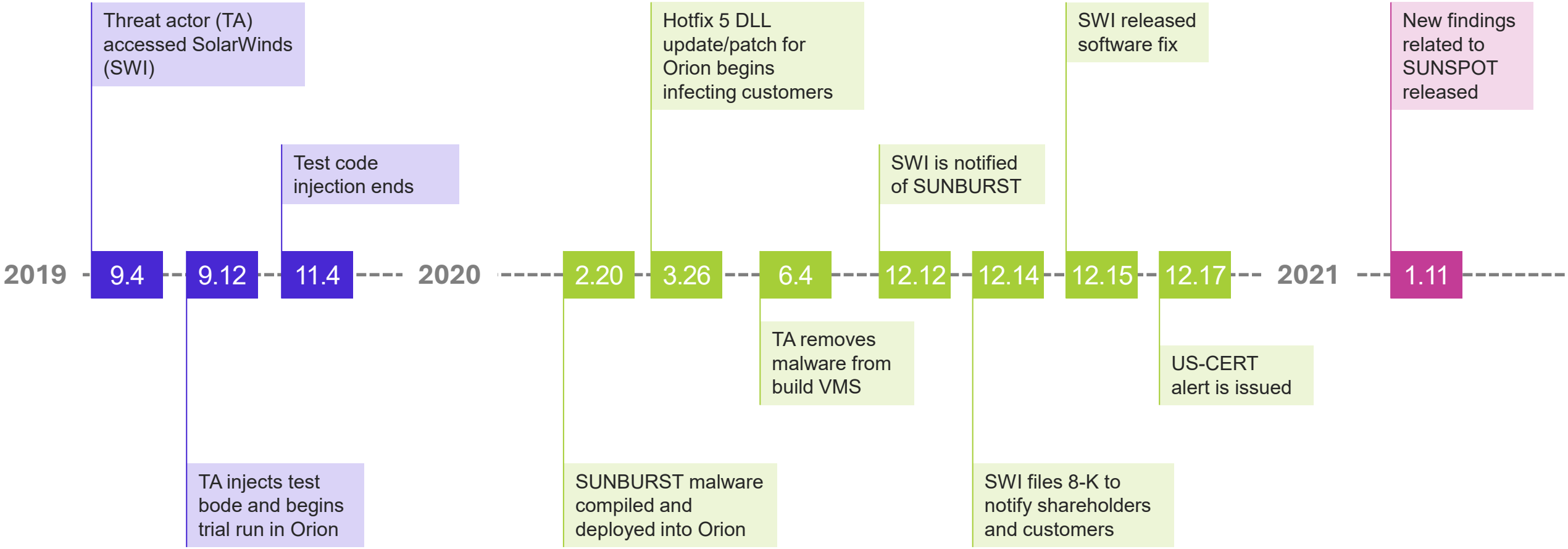
Counsel: inside legal counsel: Involve your organization's legal team promptly during incidents to navigate compliance and regulatory requirements effectively; evaluate whether you need independent legal counsel. Outside counsel should consider how to advise clients on each of these topics.

Stay informed on regulatory changes: Regularly update your knowledge on evolving cybersecurity laws and regulations to ensure ongoing compliance and readiness.

RSAC 2025 Conference

SolarWinds case chronology

SolarWinds attack timeline: overview



Source: SEC v. SolarWinds Corp., 741 F. Supp. 3d 37, 74 (S.D.N.Y. 2024), Court Opinion @ https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2023cv09518/609279/125/

Intro to law for SEC case vs. SolarWinds

Law has two important categories:

- Criminal law
- Civil law
  - Regulatory laws, actions, etc.

SolarWinds SEC case is a civil case, brought in federal court (SDNY), by a regulator (SEC)

SEC is a regulator for publicly traded companies with the goal of protecting markets and investors

- Some of the laws they enforce include:
  - Securities Act of 1933 (“Securities Act”)
  - Securities Exchange Act of 1934 (“Exchange Act”)

One aspect of investor protection is trying to ensure companies release accurate information

Some evidence basics:

- Need evidence to prove a case (and to prove a prior statement is false or misleading)
- Laws and rules of evidence apply for complaints, litigation and trial
- Statement of a party opponent
- Prior inconsistent statements

SEC focus after SolarWinds

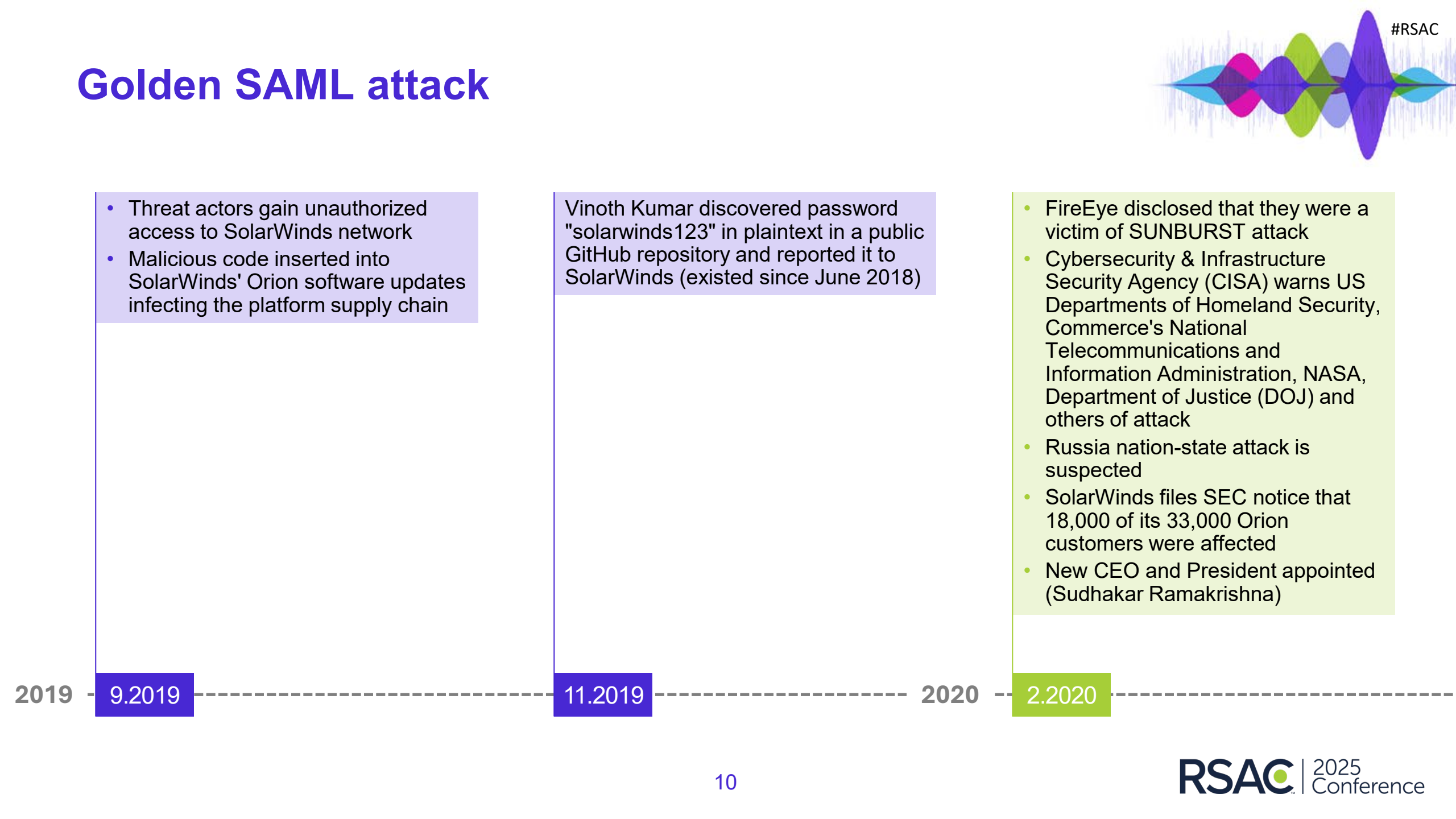
Focus on companies that make materially misleading disclosures in their SEC filings for investors regarding cybersecurity risks and intrusions

SEC took additional enforcement action in 2024: See **SEC Charges Four Companies With Misleading Cyber Disclosures**. Disclosure failures and inadequacies included:

- Downplaying the extent of their exposure to a breach by a member of the value chain
- Failing to disclose critical details about the nature and scope of any intrusions leading to a breach
- Providing generic or misleading descriptions of cybersecurity risks
- Failing in their disclosure controls and procedures

RSAC 2025 Conference

Golden SAML attack



- Threat actors gain unauthorized access to SolarWinds network
- Malicious code inserted into SolarWinds' Orion software updates infecting the platform supply chain

Vinoth Kumar discovered password "solarwinds123" in plaintext in a public GitHub repository and reported it to SolarWinds (existed since June 2018)

- FireEye disclosed that they were a victim of SUNBURST attack
- Cybersecurity & Infrastructure Security Agency (CISA) warns US Departments of Homeland Security, Commerce's National Telecommunications and Information Administration, NASA, Department of Justice (DOJ) and others of attack
- Russia nation-state attack is suspected
- SolarWinds files SEC notice that 18,000 of its 33,000 Orion customers were affected
- New CEO and President appointed (Sudhakar Ramakrishna)

Golden SAML attack

- Threat actors gain unauthorized access to SolarWinds network
- Malicious code inserted into SolarWinds' Orion software updates infecting the platform supply chain

9.2019

Vinoth Kumar discovered password "solarwinds123" in plaintext in a public GitHub repository and reported it to SolarWinds (existed since June 2018)

11.2019

2019 — 2020

- FireEye disclosed that they were a victim of SUNBURST attack
- Cybersecurity & Infrastructure Security Agency (CISA) warns US Departments of Homeland Security, Commerce's National Telecommunications and Information Administration, NASA, Department of Justice (DOJ) and others of attack
- Russia nation-state attack is suspected
- SolarWinds files SEC notice that 18,000 of its 33,000 Orion customers were affected
- New CEO and President appointed (Sudhakar Ramakrishna)

2.2020

Golden SAML attack

- SUNSPOT was identified by FireEye as a tool used to inject SUNBURST malicious code into the SolarWinds Orion software build process
- SolarWinds acknowledges “solarwinds123” password
- US intelligence agencies formally attributes attack to Russian Foreign Intelligence Service (SVR)/“Cozy Bear”
- SolarWinds hires Chris Krebs and Alex Stamos to assist with breach
- Class action lawsuit filed in Western District of Texas including Kevin B. Thompson and J. Barton Kalsu for false statements and lack of internal controls

- Patching occurs
- Congressional investigations
- Breach occurred much earlier than initially understood

2021 — 1.2021 — Through 2021

Golden SAML attack

- SUNSPOT was identified by FireEye as a tool used to inject SUNBURST malicious code into the SolarWinds Orion software build process
- SolarWinds acknowledges “solarwinds123” password
- US intelligence agencies formally attributes attack to Russian Foreign Intelligence Service (SVR)/“Cozy Bear”
- SolarWinds hires Chris Krebs and Alex Stamos to assist with breach
- Class action lawsuit filed in Western District of Texas including Kevin B. Thompson and J. Barton Kalsu for false statements and lack of internal controls

- Patching occurs
- Congressional investigations
- Breach occurred much earlier than initially understood

2021 — 1.2021 — Through 2021

Litigation developments

- SolarWinds agrees to settle shareholder class-action lawsuit for $26M (final hearing and judgment issued July 28, 2023). See SolarWinds Securities Litigation Court Documents
- Separate shareholder's derivative lawsuit was dismissed on jurisdictional grounds, and dismissal upheld on appeal. See https://courts.delaware.gov/Opinions/Download.aspx?id=347690
- SEC sends "Wells Notice" to SolarWinds corporation. See SolarWinds Form 8-K for 10/28/2022

SEC sends "Wells Notice" to former executives including CFO and CISO. See SolarWinds Form 8-K for 06/23/2023

SEC files a civil complaint against SolarWinds and CISO Timothy Brown. See https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-227.pdf

2022 — 10.28 — 2023 — 6.23 — 10.30

Original October 2023 SEC allegations

01
Ignoring serious known cybersecurity deficiencies

02
Making materially false and misleading risk disclosures in SEC filings

03
Posting misleading statements on the SolarWinds website

04
Permitting multiple internal control failures

Original October 2023 SEC allegations

01
Ignoring serious known cybersecurity deficiencies

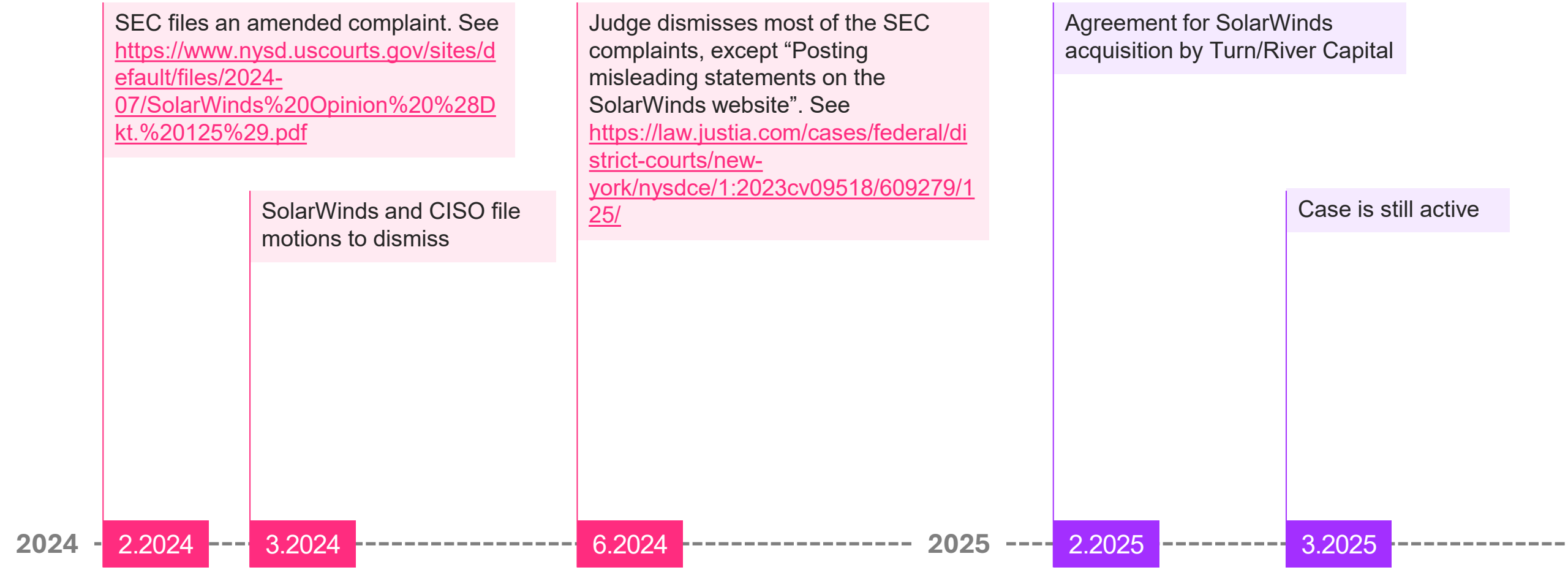
02
Making materially false and misleading risk disclosures in SEC filings

03
Posting misleading statements on the SolarWinds website

04
Permitting multiple internal control failures

RSAC 2025 Conference

Litigation status today


SEC files an amended complaint. See https://www.nysd.uscourts.gov/sites/default/files/2024-07/SolarWinds%20Opinion%20%28Dkt.%20125%29.pdf
SolarWinds and CISO file motions to dismiss
Judge dismisses most of the SEC complaints, except “Posting misleading statements on the SolarWinds website”. See https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2023cv09518/609279/125/
Agreement for SolarWinds acquisition by Turn/River Capital
Case is still active
2024
2.2024
3.2024
6.2024
2025
2.2025
3.2025

Litigation summary

Not cause to celebrate – not yet, anyway

SolarWinds made statements touting that it had strong access controls and password policies, but the court stated that:

- SolarWinds' "internal practices and discourse" … "portrayed a diametrically opposite representation for public consumption"
- The SEC complaint "amply" alleged scienter, including that the former CISO knew of the substantial body of data that impeached the security statement's content as false and misleading
- False statements on public websites can sustain securities fraud liability

This is not over

Note the updated SEC cybersecurity reporting regulations

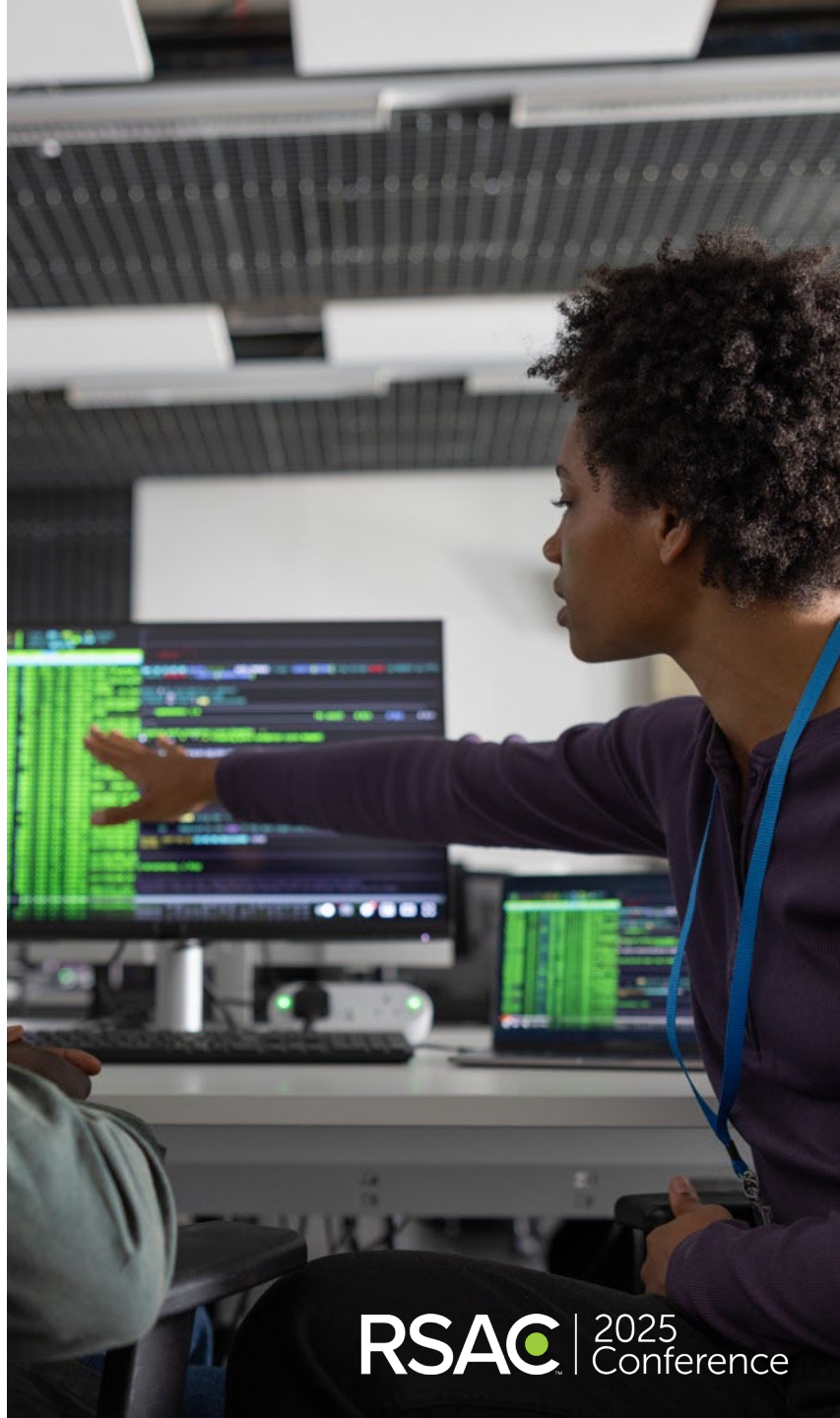
RSAC 2025 Conference

RSAC 2025 Conference

Lessons learned

Post-litigation knowledge

- Courts and SEC can hold companies liable for misrepresentations
- CISO reporting structure is crucial
- Cybersecurity is an enterprise-wide risk – all leadership levels are responsible
- Defense in depth: layered redundant defenses
- D&O insurance policies are fundamental for CISOs
- CISOs may benefit from independent legal counsel
- Educate employees on AI and emerging risks SEC cyber filings can become the basis of litigation
- CISOs should consider obtaining their own D&O policies if employer's D&O policy coverage is inadequate or does not exist



RSAC 2025 Conference

Best practices after SolarWinds

APPLY: Best Practices I

Public statements about cybersecurity must be accurate – whether aimed at investors, customers, regulators or other parties.

Companies must assess their vendors' and partners' security postures.

Vendor contracts should include security requirements and audit rights.

Must provide meaningful and accurate cybersecurity disclosures to investors.

CISOs may need to consult with corporate legal or personal legal counsel.

CISOs need to be aware of corporate marketing and public statements.

Determine if the CISO is covered under D&O policies. If not, or if any coverage provided by employer is inadequate, the CISO should consider obtaining an independent D&O policy.

APPLY: Best Practices II

All public statements about cybersecurity should be reviewed for accuracy and consistency by security and legal teams before release.

Regularly audit incident severity classifications in the incident response plan (IRP).

Determine whether the company is exhibiting “industry best practices” prior to publication on a website or other public media.

The CISO needs to have access to those with fiduciary duties, board in executive session and/or audit committee.

Consider whether separation of duties are implemented between the chief information officer (CIO)/chief technology officer (CTO) and the CISO

Escalation criteria: CISOs should engage the board to provide input on the types of incidents that should be escalated as well as incidents that should not.

Update prior risk factors and disclosures in case the company determines that a material cybersecurity incident has occurred.

RSAC 2025 Conference

Conclusions

Key insights

CISOs face increasing personal accountability in cybersecurity breaches and regulatory investigations.

Regulatory scrutiny is growing, with actions such as Wells Notices targeting individual executives, including CISOs.

Material misstatements can lead to SEC enforcement actions.

False or misleading public statements can result in liability under securities laws.

Strong internal controls and accurate public disclosures are critical.

RSAC 2025 Conference

#RSAC

Many Voices. One Community.

THANKS!

MODERATOR:

Scott M. Giordano, Esq.

Partner and Co-Founder
The CISO Law Firm PLLC
linkedin.com/in/scottmgiordano

PANELISTS:

John Bates, JD

Senior Manager, Cybersecurity
Ernst & Young LLP
linkedin.com/in/john-bates-jd

John Barker, Esq.

Partner and Co-Founder
The CISO Law Firm PLLC
linkedin.com/in/johnwbarkerii

John T. Bandler, Esq.

Principal
Bandler Law Firm PLLC
linkedin.com/in/johnbandler

RSAC 2025 Conference

The end